PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING DOCUMENTS TRANSMITTED

To:

United States Patent and Trademark
Office
Attention: Box PCT
Room 3A01, South Tower
2900 Crystal Drive
Arlington, VA 22202
United States of America

in its capacity as IPEA

Date of mailing (day/month/year)
31 March 2006 (31.03.2006)

International application No. PCT/IB2003/002847	**International filing date** (day/month/year) 18 July 2003 (18.07.2003)

Applicant
AXALTO SA et al

The International Bureau transmits herewith the following documents and number thereof:

________ copy of the international application and international search report or declaration (Administrative Instructions, Section 420)

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland** Facsimile No.: +41 22 740 14 35	Authorized officer Emmanuel Berrod Telephone No.: +41 22 338 83 38

0	**For receiving Office use only**	
0-1	International Application No.	PCT / IB 03 / 02847
0-2	International Filing Date	18 JULY 2003 (18.07.03)
0-3	Name of receiving Office and "PCT International Application"	INTERNATIONAL BUREAU OF WIPO PCT International Application

0-4	**Form - PCT/RO/101 PCT Request**	
0-4-1	Prepared using	PCT-EASY Version 2.92 (updated 01.01.2003)
0-5	**Petition** The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty	
0-6	**Receiving Office (specified by the applicant)**	International Bureau of the World Intellectual Property Organization (RO/IB)
0-7	**Applicant's or agent's file reference**	76.0724WO/PR
I	**Title of invention**	METHOD TO SECURE THE EXECUTION OF A PROGRAM AGAINST ATTACKS BY RADIATION OR OTHER
II	**Applicant**	
II-1	This person is:	applicant only
II-2	Applicant for	all designated States except US
II-4	Name	[SCHLUMBERGER SYSTEMES]^
II-5	Address:	50 AVENUE DE JAURES F-92120 MONTROUGE France
See #7		
II-6	State of nationality	FR
II-7	State of residence	FR
II-8	Telephone No.	33 1 30 08 47 81
II-9	Facsimile No.	33 1 30 08 45 24
II-10	e-mail	Patricia.Renault@sema.slb.com
III-1	**Applicant and/or inventor**	
III-1-1	This person is:	applicant only
III-1-2	Applicant for	EP: (MC)
III-1-4	Name	SCHLUMBERGER MALCO INC
III-1-5	Address:	9800 Reistertown F-MD 21117 OWING MILLS [~~France~~]^ US
^ See p1A#2		
III-1-6	State of nationality	US
III-1-7	State of residence	US

PCT/IB03/02847

III-2	**Applicant and/or inventor**	
III-2-1	This person is:	applicant and inventor
III-2-2	Applicant for	US only
III-2-4	Name (LAST, First)	GIRAUD, Nicolas
III-2-5	Address:	6 SQUARE DE BRETTEVILLE F-78150 LE CHESNAY France
III-2-6	State of nationality	FR
III-2-7	State of residence	FR
IV-1	**Agent or common representative; or address for correspondence** The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as:	common representative
IV-1-1	Name	[SCHLUMBERGER SYSTEMES] 6
IV-1-2	Address:	C/O Patricia RENAULT 36-38 rue de la Princesse BP 45 F-78431 LOUVECIENNES France
IV-1-3	Telephone No.	33 1 30 08 47 81
IV-1-4	Facsimile No.	33 1 30 08 45 24
IV-1-5	e-mail	Patricia.Renault@sema.slb.com
V	**Designation of States**	
V-1	Regional Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AP: GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW and any other State which is a Contracting State of the Harare Protocol and of the PCT EA: AM AZ BY KG KZ MD RU TJ TM and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT EP: AT BE BG CH&LI CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PT SE SI SK TR and any other State which is a Contracting State of the European Patent Convention and of the PCT OA: BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG and any other State which is a member State of OAPI and a Contracting State of the PCT

see #7

V-2	National Patent (other kinds of protection or treatment, if any, are specified between parentheses after the designation(s) concerned)	AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH&LI CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NI NO NZ OM PH PL PT RO RU SC SD SE SG SK SL TJ TM TN TR TT TZ UA UG US UZ VC VN YU ZA ZM ZW	
V-5	**Precautionary Designation Statement** In addition to the designations made under items V-1, V-2 and V-3, the applicant also makes under Rule 4.9(b) all designations which would be permitted under the PCT except any designation(s) of the State(s) indicated under item V-6 below. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit.		
V-6	**Exclusion(s) from precautionary designations**	NONE	
VI-1	**Priority claim of earlier regional application**		
VI-1-1	Filing date	18 July 2002 (18.07.2002)	
VI-1-2	Number	02291812.2	
VI-1-3	Regional Office	EP	
VII-1	**International Searching Authority Chosen**	European Patent Office (EPO) (ISA/EP)	
VII-2	**Request to use results of earlier search; reference to that search**		
VII-2-1	Date	17 December 2002 (17.12.2002)	
VII-2-2	Number	EP02291812.2	
VII-2-3	Country (or regional Office)	EP	
VIII	**Declarations**	Number of declarations	
VIII-1	Declaration as to the identity of the inventor	-	
VIII-2	Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent	-	
VIII-3	Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application	-	
VIII-4	Declaration of inventorship (only for the purposes of the designation of the United States of America)	- 1 A	
VIII-5	Declaration as to non-prejudicial disclosures or exceptions to lack of novelty	-	

A
RO

PCT/IB03/02847

~~[4/4]~~ 5/5 ▲

PCT REQUEST

76.0724WO/PR

Original (for **SUBMISSION**) - printed on 18.07.2003 10:33:01 AM

IX	Check list	number of sheets	electronic file(s) attached
IX-1	Request (including declaration sheets)	~~[4]~~ ▲ 5 ▲	-
IX-2	Description	7	-
IX-3	Claims	3	-
IX-4	Abstract	1	EZABST00.TXT
IX-5	Drawings	1	-
IX-7	TOTAL	~~[16]~~ ▲ 17 ▲	
	Accompanying items	paper document(s) attached	electronic file(s) attached
IX-8	Fee calculation sheet	✓	-
IX-11	Copy of general power of attorney	reference no. <no.>GPA 01/0269	-
IX-11	Copy of general power of attorney	reference no. <no.>GPA 02/359	-
IX-17	PCT-EASY diskette	-	Diskette
IX-18	Other (specified):	DECLARATION OF INVENTORSHIP	-
IX-19	**Figure of the drawings which should accompany the abstract**	2	
IX-20	**Language of filing of the international application**	English	
X-1	**Signature of applicant, agent or common representative**		
X-1-1	Name	SCHLUMBERGER SYSTEMES	
X-1-2	Name of signatory	Patricia RENAULT	
X-1-3	Capacity	Agent of the Common Representative	

▲ RO

FOR RECEIVING OFFICE USE ONLY

10-1	**Date of actual receipt of the purported international application**	18 JULY 2003 (18.07.03)
10-2	**Drawings:**	
10-2-1	Received	
10-2-2	Not received	
10-3	**Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application**	
10-4	**Date of timely receipt of the required corrections under PCT Article 11(2)**	
10-5	**International Searching Authority**	ISA/EP
10-6	**Transmittal of search copy delayed until search fee is paid**	

FOR INTERNATIONAL BUREAU USE ONLY

11-1	**Date of receipt of the record copy by the International Bureau**	28 AOUT 2003

ABSTRACT

The method according to this invention concerns a method to secure the execution of a program stored in an electronic assembly comprising information processing means and information storage means. The method consists in checking the execution time of at least one sequence in said program with respect to the normal predetermined execution time of said sequence.

This invention also concerns the electronic module in which said method is implemented and the card comprising said module.

Figure of the abstract: Fig. 2

ATENT COOPERATION TREATY

PCT

19/d

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 76.0724WO/PR	**FOR FURTHER ACTION** see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/IB 03/02847	International filing date *(day/month/year)* 18/07/2003	(Earliest) Priority Date *(day/month/year)* 18/07/2002
Applicant SCHLUMBERGER SYSTEMES		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 4 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language,** the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readble form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

4. With regard to the **title,**

☐ the text is approved as submitted by the applicant.

☒ the text has been established by this Authority to read as follows:

METHOD TO SECURE THE EXECUTION OF A PROGRAM AGAINST ATTACKS

5. With regard to the **abstract,**

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 2

☒ as suggested by the applicant.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

☐ None of the figures.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 03/02847

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F11/00 G07F7/10 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	FR 2 707 409 A (SOLAIC SA) 13 January 1995 (1995-01-13) the whole document ---	1-3,6,7, 10-12
X	US 5 892 900 A (GINTER KARL L ET AL) 6 April 1999 (1999-04-06) column 243, line 64 -column 244, line 43; figures 69K-N ---	1,2,5, 10,13
A	US 2001/016910 A1 (TAKAHASHI MASATOSHI ET AL) 23 August 2001 (2001-08-23) page 6, left-hand column, line 8 - line 56; figure 15 ---	8
A	FR 2 795 836 A (BULL CP8) 5 January 2001 (2001-01-05) the whole document --- -/--	1-12

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 17 December 2003	Date of mailing of the international search report 05/01/2004
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Absalom, R

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 03/02847

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 3 723 975 A (KURTZ H ET AL) 27 March 1973 (1973-03-27) claim 1 ---	1,10
A	US 4 710 613 A (SHIGENAGA YOSHIMI) 1 December 1987 (1987-12-01) abstract ---	1,10
A	US 3 426 331 A (JOYCE THOMAS F) 4 February 1969 (1969-02-04) claim 1 -----	1,10

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 03/02847

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2707409 A	13-01-1995	FR 2707409 A3	13-01-1995
US 5892900 A	06-04-1999	AU 4170397 A	19-03-1998
		CA 2265473 C	22-10-2002
		CA 2373508 A1	05-03-1998
		CA 2373542 C	12-11-2002
		EP 0922248 A1	16-06-1999
		US 2003191719 A1	09-10-2003
		WO 9809209 A1	05-03-1998
		US 2003163431 A1	28-08-2003
US 2001016910 A1	23-08-2001	JP 2001195555 A	19-07-2001
		JP 2001266103 A	28-09-2001
		TW 536672 B	11-06-2003
		US 2001047480 A1	29-11-2001
FR 2795836 A	05-01-2001	FR 2795836 A1	05-01-2001
US 3723975 A	27-03-1973	DE 2230119 A1	25-01-1973
		FR 2144222 A5	09-02-1973
		GB 1360566 A	17-07-1974
		JP 52044495 B	08-11-1977
US 4710613 A	01-12-1987	JP 1825638 C	28-02-1994
		JP 5033416 B	19-05-1993
		JP 61139873 A	27-06-1986
		AT 61680 T	15-03-1991
		CA 1245764 A1	29-11-1988
		DE 3582131 D1	18-04-1991
		EP 0186038 A2	02-07-1986
		FR 2574963 A1	20-06-1986
US 3426331 A	04-02-1969	NONE	

**Declaration of inventorship (Rules 4.17(iv) and 51 *bis*.1(a)(iv))
for the purposes of the designation of the United States of America:**

I hereby declare that I believe I am the original, first and sole (if only one inventor is listed below) or joint (if more than one inventor is listed below) inventor of the subject matter which is claimed and for which a patent is sought.

This declaration is directed to the international application of which it forms a part.

I hereby declare that my residence, mailing address, and citizenship are as stated next to my name.

I hereby state that I have reviewed and understand the contents of the above-identified international application, including the claims of said application. I have identified in the request of said application, in compliance with PCT Rule 4.10, any claim to foreign priority, and I have identified below, under the heading "Prior Applications," by application number, country or member of the World Trade Organization, day, month and year of filing, any application for a patent or inventor's certificate filed in a country other than the United States of America, including any PCT international application designating at least one country other than the United States of America, having a filing date before that of the application on which foreign priority is claimed.

Prior Applications:

I hereby acknowledge the duty to disclose information that is know by me to be material to patentability as defined by 37C.F.R. § 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the PCT international filing date of the continuation-in-part application..

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name: Nicolas GIRAUD
Residence: LE CHESNAY - FRANCE
(city and country)
Mailing Address: SCHLUMBERGER SYSTEMES INTELLECTUAL PROPERTY DEPARTMENT
36-38 Rue de la Princesse BP 45
78431 LOUVECIENNES CEDEX - FRANCE
Citizenship: FRENCH
Inventor's signature: Date:18 July 2003

Name:
Residence:
(city and country)
Mailing Address:
Citizenship:
Inventor's signature: Date:

Name:
Residence:
(city and country)
Mailing Address:

Citizenship:
Inventor's signature: Date:

□ This declaration is continued on the following sheet, "Continuation of Box No. VIII (iv)".

METHOD TO SECURE THE EXECUTION OF A PROGRAM AGAINST ATTACKS BY RADIATION OR OTHER

This invention concerns a method and a device to secure an electronic assembly implementing a program to be protected. More precisely, the purpose of the method is to propose a defence against attacks by radiation, flash, light or other and more generally against any attack disturbing the execution of the program instructions.

TECHNICAL FIELD

When executing a program, attacks by radiation modify the instruction codes executed by the processor. The program instructions are replaced by inoperative instructions. Consequently, certain sections of the code fail to execute or execute irregularly, for example the execution of inoperative instructions instead of a security processing sequence.

This applicant filed a French patent application No. 0016724 on 21 December 2000 concerning a method to secure the execution of a program stored in a microprocessor controlled electronic module, as well as the associated electronic module and integrated circuit card. The prior art described in said application applies to this invention. The solution protected in said application consists in triggering interrupts intermittently and thereby diverting the program execution to protect against possible attacks. This solution offers a good probability of detecting and preventing the attacks by radiation. However, some attacks may not be detected, especially if the attack occurs briefly between two interrupts.

One purpose of this invention is to propose efficient protection even for very short attacks.

Another purpose of this invention is to propose a solution which could be implemented in the current components without adaptation, which consumes few resources and which does not reduce the performance of the assembly in which it is implemented.

SUMMARY OF THE INVENTION

This invention concerns a method to secure the execution of a program in an electronic assembly comprising information processing means and information storage means, characterised in that it consists in checking the execution time of at least one sequence of said program with respect to the normal predetermined execution time of said sequence.

This invention also concerns an electronic module in which said method is implemented, a card comprising said module and a program to implement said method.

BRIEF DESCRIPTION OF THE DRAWINGS

Other purposes, features and advantages of the invention will appear on reading the description which follows of the implementation of the method according to the invention and of a mode of realisation of an electronic system designed for this implementation, given as a non-limiting example, and referring to the attached drawings in which:

- figure 1 is a diagrammatic representation of a mode of realisation of an electronic module according to this invention;
- figure 2 is a diagrammatic representation of part of the module according to figure 1 in which the steps of the method according to this invention have been indicated.

WAY OF REALISING THE INVENTION

The purpose of the method according to the invention is to secure an electronic assembly and for example an onboard system such as a smart card implementing a program. The electronic assembly comprises at least a processor and a memory. The program to be secured is installed in the memory, for example ROM type, of said assembly.

As a non-limiting example, the electronic assembly described below corresponds to an onboard system comprising an electronic module 1 illustrated on figure 1. This type of module is generally realised as a monolithic integrated electronic microcircuit, or chip, which once physically protected by any known means can be assembled on a portable object such as for example a smart card, integrated circuit card or other card which can be used in various fields.

The microprocessor controlled electronic module 1 comprises a microprocessor CPU 3 with two-way connection via an internal bus 5 to a non volatile memory 7 of type ROM, EEPROM Flash, FeRam or other containing the program PROG 9 to be executed, a random access memory (RAM) 11, input/output (I/O) means 13 to communicate with the exterior and means 15 TIMER to evaluate the program execution time such as a counter with triggering of an interrupt on expiry. An exception is raised when the counter 15 expires. The exception is followed by diversion of the program code to an interrupt processing routine (ROUTINE – figure 2).

Traditionally, the microprocessor central processing unit CPU 3 illustrated on figure 1 comprises in particular an arithmetic and logic unit UAL 16, a program counter register CO 17 giving the address of the next instruction to be executed, a stack pointer register PP 18 giving the memory address of the top of the stack.

On CISC (Complex Instruction Set Computer) type components for smart card, the execution time of a sequence of instructions is the sum of the execution times of each instruction executed. The execution time of an instruction generally varies between 2 and 11 clock cycles. The execution of a sequence of instructions is characterised by the points of departure and arrival and the path followed, which is likely to include loops and branches.

Attack by radiation converts any instruction of variable execution time into an inoperative instruction of fixed execution time such as, for example, a NOP instruction (2 clock cycles on the SLE66 cards) or a BTJT instruction (5 clock cycles on the ST19 cards). The sequence attacked is converted into a "linear" sequence which consists in executing a series of inoperative instructions with incrementation of the program counter 17 CO with no loops or branches. The path followed is therefore modified and the point of arrival after the normal execution time will be different from that of the normal point of arrival. Even with a very short attack, the execution time of a sequence is changed slightly and the point of arrival after the normal execution time is different from that planned.

The method according to the invention consists in checking the execution time of at least one sequence S of the program 9 with respect to its normal predetermined execution time, which is invariable if there is no disturbance, and more precisely in checking that the execution of sequence S is at the planned point of arrival after the normal predetermined execution time T of said sequence. The check may concern, for example, one or more sensitive instruction sequences which require greater protection such as the cryptographic algorithms, the security processes or other.

As shown on figure 2 (step (1)), the counter TIMER 15 is started at the point of departure of execution of sequence S with an initialisation value corresponding to the normal execution time T of the processing concerned. A counter initialisation code INIT is added before the start of each sequence S to be protected.

The initialisation value is predetermined during development and must be constant: it must not vary during normal execution conditions. The interrupts likely to occur during execution of the interrupt are therefore deactivated, as well as the mechanisms designed to modify consumption during a processing operation (variation of the number of instruction cycles or introduction of additional cycles). If the sequence S includes branches, all execution paths must lead, on expiry of the processing execution time, to the same point of arrival, i.e. to the same instruction and more precisely to the same value of the program counter CO 17. The time of execution through each branch must therefore be equalised by adding null instructions such as for example NOP instructions. The processing duration is therefore the same no matter which branch is followed. Similarly, if the sequence S includes loops of variable execution time, resynchronisation loops must be added to compensate for the variations so that the total execution time remains constant.

A variable accessible by the counter interrupt processing routine is initialised with the value of the program counter CO 17 corresponding to the value expected at the normal point of arrival of the sequence S to be protected. On expiry of the counter 15 TIMER, an interrupt is raised (step (2), fig. 2). The value of the program counter CO corresponds to the actual point of arrival: this value is saved at the address given by the stack pointer PP 18 and the code execution is diverted to the interrupt processing routine ROUTINE stored in ROM and/or in EEPROM and/or any non volatile memory (step (3)). The interrupt routine ROUTINE reads the value of the program counter CO at the end of normal execution time on the stack and checks that it corresponds to the expected value sent by variable as seen previously.

If the sequence has reached the planned point of arrival after the normal execution time, the interrupt processing routine ends and plans a normal return to the program diversion point (step (4)): program execution continues normally. Otherwise, disturbance in the execution of program sequence S is observed and an attack by radiation is detected. Various measures can then be taken such as, for example, interruption of program execution, setting of a fraud indicator (INDIC - step (4')) in non volatile memory 7 to indicate that a fraudulent attack has taken place and for example to prohibit any future use of the operating system.

To guarantee maximum efficiency, the point of arrival should only be reached once during execution of the sequence. If the sequence passes the point of arrival several times, there is a probability that execution of the sequence is at the point of arrival planned on expiry of the counter but not real considering the number of passages via the point of arrival, even if an attack by radiation has occurred and modified the sequence execution.

In the special case of RISC (Reduced Instruction Set Computer) components, most instructions are executed in one clock cycle.

Consequently, if an attack by radiation substitutes for any instructions executing in one clock cycle inoperative instructions also executing in one clock cycle, it does not change the sequence execution time and the point of arrival remains the same: the attack cannot be detected. To guarantee detection in this special case, the method according to the invention consists in adding one or more short null loops in the code. The loops added increase the normal execution time of the instruction sequence to be protected. In the event of attack by radiation, the loops disappear and the sequence execution time is modified, so the attack can be detected.

Triggering of the processing on expiry of the counter is based on a hardware means which can withstand attacks by radiation.

Note that execution of the interrupt processing routine can be disturbed by an attack by radiation. According to a development of the invention, the method according to this invention is improved by placing the interrupt return instruction at the last memory location or just before a shared domain boundary. If an attack by radiation prevents execution of the interrupt return, the program counter CO is incremented at the next memory location which is outside the permitted program memory area. A procedure specific to the component is then carried out, for example on component ST19, generation of a non maskable interrupt (NMI) with reset. According to another additional development of the invention, a sequence to set a fraud indicator is introduced in non volatile memory after the interrupt return instruction.

Consequently, the method according to this invention can be used to detect any attack by radiation, irrespective of its duration, on a protected sequence. Said method is very economical in terms of resources and execution time. In terms of resources, the method only requires the addition of counter initialisation code, counter interrupt management routine code and possibly code to equalise the execution branches and resynchronise the loops. The execution time consumed by the method according to the invention for each protected instruction sequence corresponds to counter initialisation, execution of the interrupt processing routine and the code possibly added to equalise branches and resynchronise loops. The method can therefore be used to protect the code without reducing the performance in terms of code size and execution time. The method uses a counter with associated interrupt.

In addition, the choice of a counter with triggering of interrupt on expiry offers several advantages. Firstly, it is part of the basic equipment of microprocessor controlled electronic modules. Secondly, the programming involved is quite easy. It therefore represents a very simple and very reliable hardware means of triggering an interrupt without software intervention.

The method according to the invention can also be used to propose a defence against any attack unpredictably modifying an instruction sequence such as the DFA (Differential Fault Analysis) attack or other (unexpected jumps, modification or disturbance of the logic associated with the program counter CO, conversion of one instruction into another).

CLAIMS

1- Method to secure the execution of a program in an electronic assembly comprising information processing means and information storage means, characterised in that it consists in checking the execution time of at least one sequence of said program with respect to the normal predetermined execution time of said sequence.

2- Method according to claim 1, characterised in that it consists in checking during the execution of at least one sequence of said program that the execution time of said sequence corresponds to the normal predetermined execution time of said sequence.

3- Method according to claim 1 or 2, characterised in that it consists in checking the point of arrival of said sequence on expiry of the normal predetermined execution time of said sequence.

4- Method according to one of claims 1 to 3, characterised in that it consists in checking that the execution of said sequence is at the planned point of arrival on expiry of the normal predetermined execution time of said sequence.

5- Method according to one of claims 1 to 4, characterised in that it consists in checking the execution time of at least one sequence of said program with respect to the normal predetermined execution time of said sequence so as to protect against attacks disturbing the execution of said program.

6- Method according to one of claims 1 to 5, characterised in that it consists in triggering at the start of said sequence an interrupt counter initialised to the value of the normal predetermined execution time of said sequence, in triggering an interrupt in the program execution on expiry of the counter and in diverting execution of said program to an interrupt management routine in order to check the point of arrival of said sequence.

7- Method according to one of the previous claims, characterised in that if the execution time of said sequence is not normal, the interrupt management routine is immediately followed by a sequence to set a fraud indicator in memory or by an interruption of the current execution by another means.

8- Method according to one of the previous claims, characterised in that it consists in adding to said sequence instructions or loops or equivalent so as to equalise the execution time of the sequence in all its branches or so that the execution time of said sequence is modified if there is an attack.

9- Method according to claim 6, characterised in that the interrupt management routine is placed at the last location of the program memory or just before a shared domain boundary so as to leave the permitted program memory area if an attack prevents execution of the interrupt return.

10- Electronic module comprising information processing means and information storage means containing a program to be executed, characterised in that it comprises means to check the execution time of at least one sequence of said program with respect to the normal predetermined execution time of said sequence.

11 – Module according to claim 10, characterised in that the means comprise a counter with triggering of an interrupt on expiry.

12- Card characterised in that it comprises the electronic module according to claim 10 or 11.

13 - Computer program including program code instructions to execute steps of the method according to one of claims 1 to 9 when said program is run in a computer system.

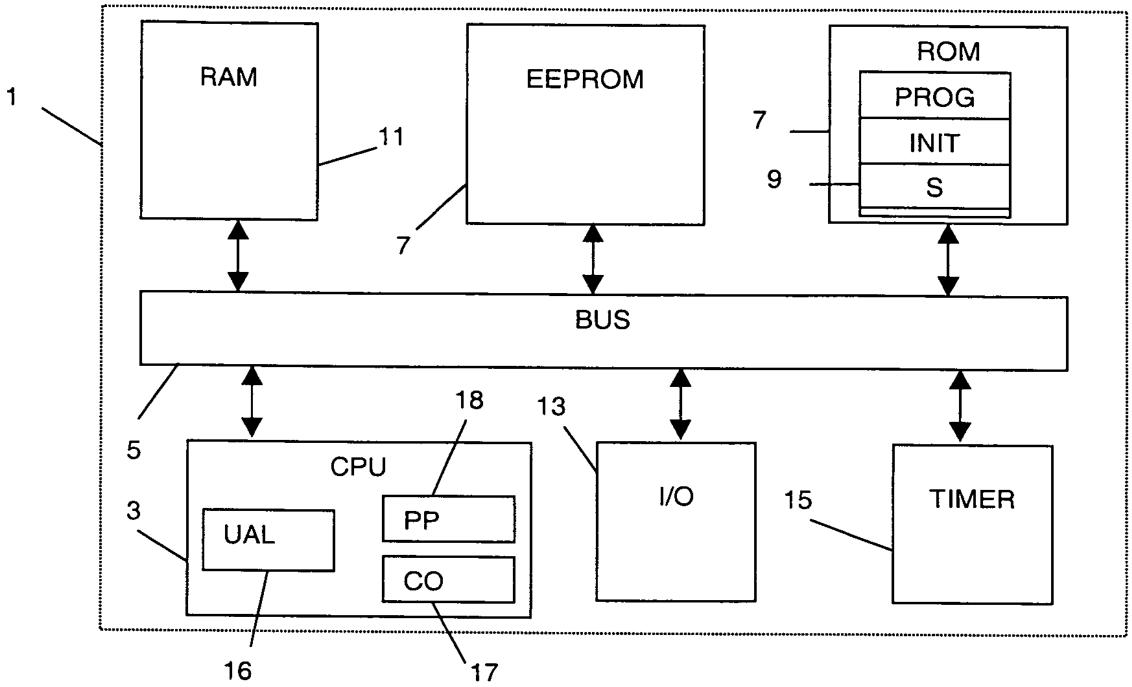
1
RAM
11
EEPROM
7
ROM
PROG
INIT
S
7
9
BUS
5
CPU
3
UAL
PP
CO
18
16
17
13
I/O
15
TIMER

FIG. 1

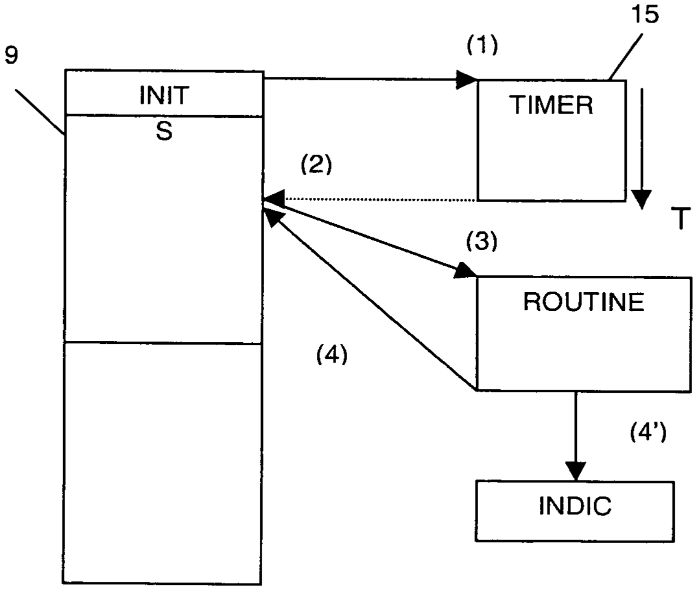
9
INIT
S
(1)
15
TIMER
T
(2)
(3)
ROUTINE
(4)
(4')
INDIC

FIG. 2